REMARKS

Favorable reconsideration and allowance are respectfully requested in view of the following remarks. Claims 1-10 are currently pending in the present application.

Rejection Under 35 U.S.C. §102(e)

Claims 1-10 are rejected under 35 U.S.C. § 102(e) as being anticipated by Edgett et al. (U.S. Patent Publication No. 2004/0034771; hereinafter "Edgett"). This rejection is respectfully traversed.

Edgett describes a system for changing encryption information in a computer network. The system provides network security by using a public/private key pair. A network user credential may be encrypted with a public key prior to transmitting the information to a server. The server then decrypts the network user credential using the private key. The decrypted network user credential is verified by an authentication server (see paragraphs 0047-0050, Edgett). However, Edgett fails to teach each and every feature of the present invention as recited in independent claims 1, 4 and 7-10.

Independent claim 1 is directed to an authenticated device. The authenticated device as recited in claim 1 comprises:

> a memory unit to store at least one algorithm identifier and at least one encryption key identifier;
>
> a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device;
>
> a receiving unit to receive from the authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit; and
>
> an authentication processing unit to perform an authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit.

Edgett fails to disclose a receiving unit to receive from the authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit as in the present invention. Instead, Edgett is directed to a dialup network

to update encryption algorithm used in network access security. Specifically, after a user has successfully performed a dialup access to a network and if there is an algorithm/key update required, then the new algorithm/key is downloaded to the user's computer. However, contrary to the assertion by the Examiner, the updated algorithm and key are not a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit as in the present invention. Thus, Edgett neither teaches nor suggests "a receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit" as recited in claim 1.

Independent claim 4 is directed to an authenticating device. The authenticating device as recited in claim 4 comprises:

> a memory unit to store at least one algorithm identifier and at least one encryption key identifier;
>
> a receiving unit to receive at least one algorithm identifier and at least one encryption key identifier from an authenticated device;
>
> a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit;
>
> a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device; and
>
> an authentication processing unit to perform an authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit.

Edgett fails to disclose a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit as in the present invention. Edgett, on the other

hand, is merely concerned with storing private key in the server for decrypting user credential information to grant or deny network access to a dialup computer user. Contrary to the Examiner's assertion, storing private key is not selecting a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit as in the present invention. Thus, Edgett neither teaches nor suggests "a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit" as recited in claim 4.

Independent claim 7 recites, *inter alia*, "a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step; a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device; a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device". It is demonstrated above that Edgett fails to teach or suggest the recited features for the reasons discussed with respect to claims 1 and 4.

Furthermore, Edgett is merely concerned with a dialup computer, which sends encrypted user credential to a server for gaining access to a network. If there is an updated key/algorithm, the server then sends the updated key/algorithm to the dialup computer. Therefore, a single set of key/algorithm is being communicated between the dialup computer and the server. Thus,

Edgett does not teach or suggest "a first transmitting step to transmit, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored; a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier" as recited in claim 7.

Independent claim 8 recites, *inter alia*, "a first receiving step to receive the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device by the first transmitting step, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers; a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step; a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device; a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device". It is demonstrated above that Edgett fails to teach or suggest the recited features for the reasons discussed with respect to claims 1, 4 and 7.

Independent claim 9 recites, *inter alia*, "transmitting, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored; receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier; selecting, at the

authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received; transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device; receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device". It is demonstrated above that Edgett fails to teach or suggest the recited features for the reasons discussed with respect to claims 1, 4 and 7.

Independent claim 10 recites, *inter alia*, "transmitting, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored; receiving the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers; selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received; transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device; receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device". It is demonstrated above that Edgett fails to teach or suggest the recited features for the reasons discussed with respect to claims 1, 4 and 7.

In view of the above remarks, it is respectfully submitted that Edgett does not anticipate independent claims 1, 4 and 7-10. As claims 2, 3, 5 and 6 are dependent to claims 1 and 4

respectively, it is respectfully submitted that these claims are also patentable for at least the same reasons discussed with respect to claims 1 and 4. Thus, it is respectfully submitted that these rejections should be withdrawn.

CONCLUSION

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Dennis P. Chen Reg. No. 61,767 at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Dated: December 19, 2008

Respectfully submitted,

By _____

D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant